Security Policies and Middleware in OSG

June 18, 2007
JRA1 All Hands Meeting

Gabriele Garzoglio
Computing Division, Fermilab

Open Science Grid

Overview

- OSG Security
  - courtesy Don Petravick
- Access Control and Privileges
- Auditing
  - courtesy Tanya Levshina

Open Science Grid

OSG Security

- OSG Proposal: "We propose to build a cyber-infrastructure that can grow to provide thousands of users effective access to 100,000 CPUs, 10s of PB of storage, located at hundreds of sites and interconnected by multiple 10Gb/s network links."
- Technical Basis:
  - Service-based access to compute and storage services.
  - A software stack used by experiments to manage their users and their jobs.
  - The environment interoperates with other similar grid environments
    - LCG, Teragrid, et al.

Open Science Grid

OSG Capacity Targets

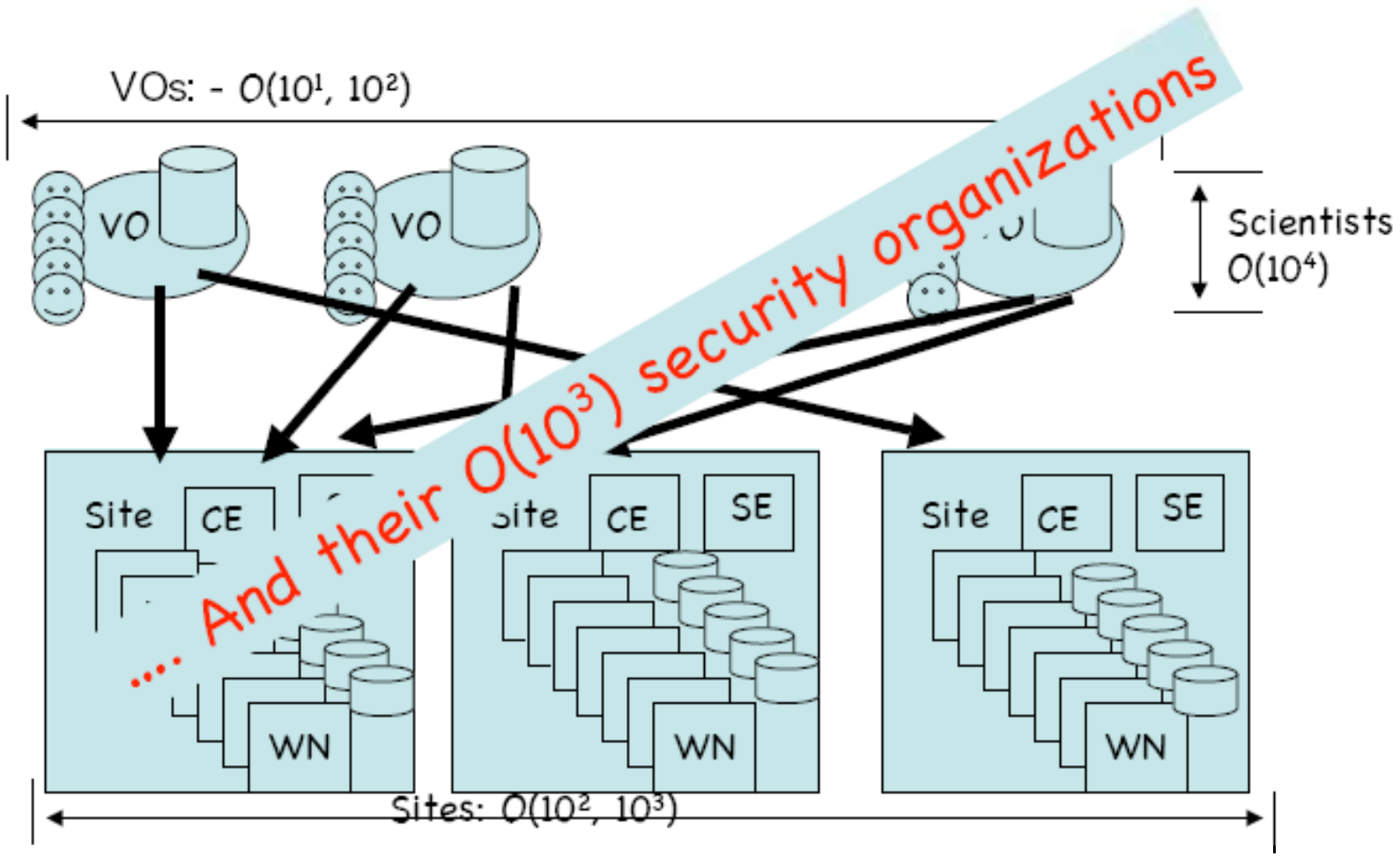
MSI2000 ◄——————————► Petabytes ◄——————————►

Org	2006	2007	2008	2009	2006	2007	2008	2009
ATLAS	3	5	14	24	1.1	2.6	7.6	11.8
CMS	4	8	16	22	1.0	2.5	4.5	4.9
LIGO	4	5	6	6	0.2	TBD	TBD	TBD
STAR	2	3	6	12	0.04	0.06	0.1	0.2
other	10	13	17	22	1.0	1.0	1.4	1.9
Total	**23**	**34**	**59**	**86**	**3.3**	**6.1**	**13.6**	**18.8**

In 2008 we estimate: 53 MSI2K = 26,000 CPUs; 74 MSI2K = 37,000 CPUs;

Open Science Grid

Me, My Friends, the Grid



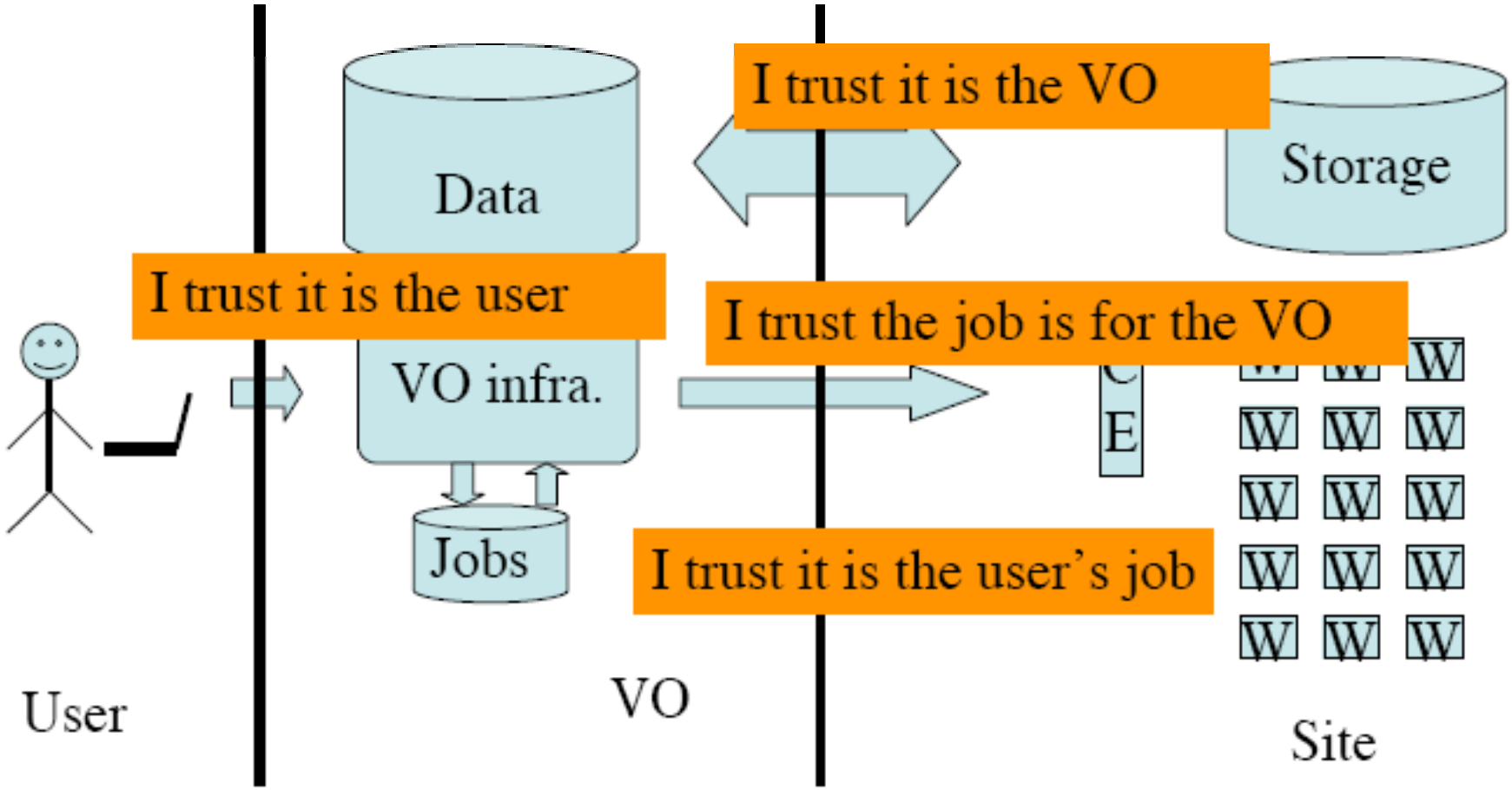
Open Science Grid

Grid Security

- The goal of grid security is establish trust that computing organized along these lines will have appropriate integrity, availability, and confidentiality.
- OSG cannot bear the security responsibilities of sites or VO's.
- Therefore, initially, inter-entity security is conceptually a set of pair-wise agreements.
  - We have more than a few autonomous parties
  - Not a small task.

Open Science Grid

Illustrative example



Operational Grid Security

- Based on NIST model – Controls based on risk, rooted in policy.
  - Risk = f(vulnerability, threat)
  - Goal: Achieve acceptable risk
    - Recall -- context is open science.
  - Means: Controls
    - Management (what did we decide?)
    - Operational (we count on behaviors)
    - Technical (stuff done in HW/SW)

Open Science Grid

Some Specifics

- OSG security seeks to compliment, not replace site and VO security organizations.
  - Recall Roadmap: $O(10^4)$ parties. Now: $O(10^3)$
    - Make the security discussion scalable by standardizing the many elements of the discussion.
  - Foster a secure software stack for grid services.
  - Foster communications
  - Know what's going on from the perspective of the whole grid

Open Science Grid

Scaling

- Make the discussion standard.
  - Think of the market in mortgages
    - Many standard terms
- Model security policies
  - JSPG: sites, VOs, users.
  - IGTF: Identity providers.
  - TBD:
    - Service providers (likely JSPG)
    - Software providers.

Open Science Grid

Overview

- ✓OSG Security
  - courtesy Don Petravick
- ➢Access Control and Privileges
- Auditing
  - Courtesy Tanya Levshina

VO Services Project Charter

- The project provides an infrastructure to manage user registration and implement fine-grained authorization to access rights on computing and storage resources.
- Authorization is linked to identities and extended attributes. Mapping is dynamic and supports pool accounts. Enforcement of access rights is implemented using UID/GID pairs.
- The infrastructure aims at reducing administrative overhead. Authorization service is central at the site.
- The project is responsible for the development and maintenance of the infrastructure and for assisting with the deployment and support on the OSG.

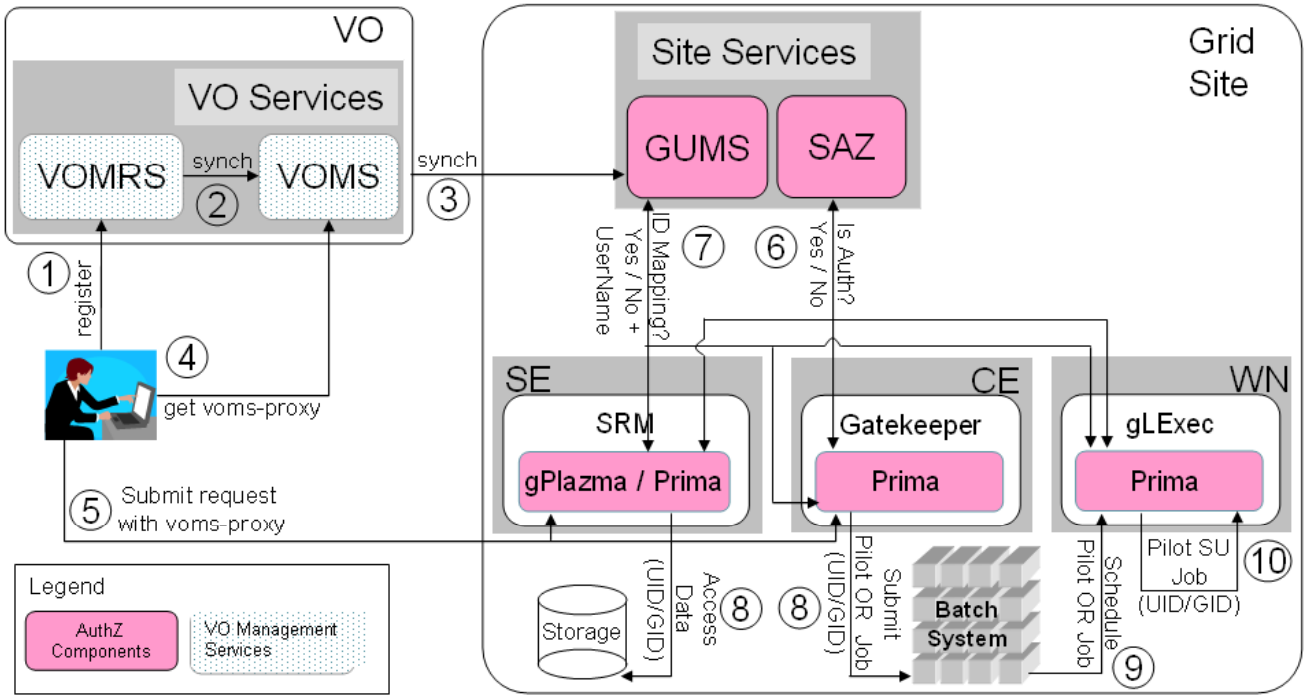
Open Science Grid

Stakeholders

- Stakeholders giving requirements: US CMS and US ATLAS.
- Joint Project of Fermilab, BNL, PPDG, Virginia Tech, UCSD, OSG since 2003
- Different institutions are responsible for the maintenance of different components
- Core software distributed via VDT

VO Services Architecture

- User identity and attributes are maintained in VOMS through VOMRS
- Users interact with VOMS to get attribute-enhanced credentials
- Gateway software (**CE and SE**) performs
  - identity mapping call-out through the PRIMA module
  - access control call-out through the SAZ module
- GUMS server maintains identity / attribute mapping **for all the gateways at a site**
- gPlazma server enhances UID/GID mapping with service-specific parameters (e.g. root path for SE).
- SAZ checks black/white lists
- Periodically, GUMS synchronizes with VOMS users/groups



Open Science Grid

Deployment on OSG

- The authorization system (GUMS) has been deployed at O(10) sites
  - US CMS T2 centers and T1 at FNAL
  - US ATLAS T2 centers and T1 at BNL
  - FermiGrid (includes SAZ) et al.
- US CMS, US ATLAS, and DZero have defined roles that are implemented using VOMS. Sites configure GUMS (PDP) to implement local identity mapping

Closing Project Phase II

Deliverable of Phase II are due in the time scale of OSG V0.8.0 release (Aug 07):

- Document current use of credential attributes
- GUMS v1.2
- LIGO Authentication Requirements
- gLExec deployment for CDF/CMS
  - Being packaged in VDT.
- gPlazma
  - Deployment underway. Further development and maintenance part of dCache project.
  - Storage role/access requirements part of Phase III
- VOMRS 1.3. Part of VDT release 1.6.1 in May 2006.
  - CERN (01/07), Fermilab (04/07), APAC (11/06)

Open Science Grid

Goals for Phase III ? (1)

- Interface/integrate/migrate OSG AuthZ components more into emerging standards.
- Set path for less effort in the future
- Prepare for use of new AuthN mechanisms (ie Shiboleth).
- VOMRS
  - Interface to Shib; Use more standard workflow engine, persistency, UI technology
- Accounting integration : Interface roles GRAM-Auditing and Gratia

Open Science Grid

Goals for Phase III ? (2)

- Support finer-grain access to Storage
  - SRM/dCache does not manage privileges directly via X509 credential attributes. UID, GID, Root Path, … mappings are required.
  - Stakeholders are interested in supporting combinations of read / write accesses to files / directories by VO, VO groups, and group roles.
- Improve software stack validation and regression tests across releases.
- Ongoing OSG - EGEE AuthZ interoperability. Already started:
  - Globus develops the common library (based on XACML2/SAML2): prototype version in collaboration w/ IBM on Apr 07.
  - Understanding and feeding back OSG and EGEE requirements: implementation of some key features estimated for July 07
  - Holding regular meetings (Oct 06, Feb 07, Mar 07, Apr 07, Jun 07)

Open Science Grid

What about Policy ?

- Currently no mechanism to define VO authorization policies and apply them consistently across sites.
  - SBIR Phase I grant approved
  - GPBox ?
- More maintainable authentication management by implementing certificate validation service site-centralized.

Open Science Grid

Overview

- ✓ OSG Security
  - courtesy Don Petravick
- ✓ Access Control and Privileges
- ➢ Auditing
  - Courtesy Tanya Levshina

Open Science Grid

Project Motivations

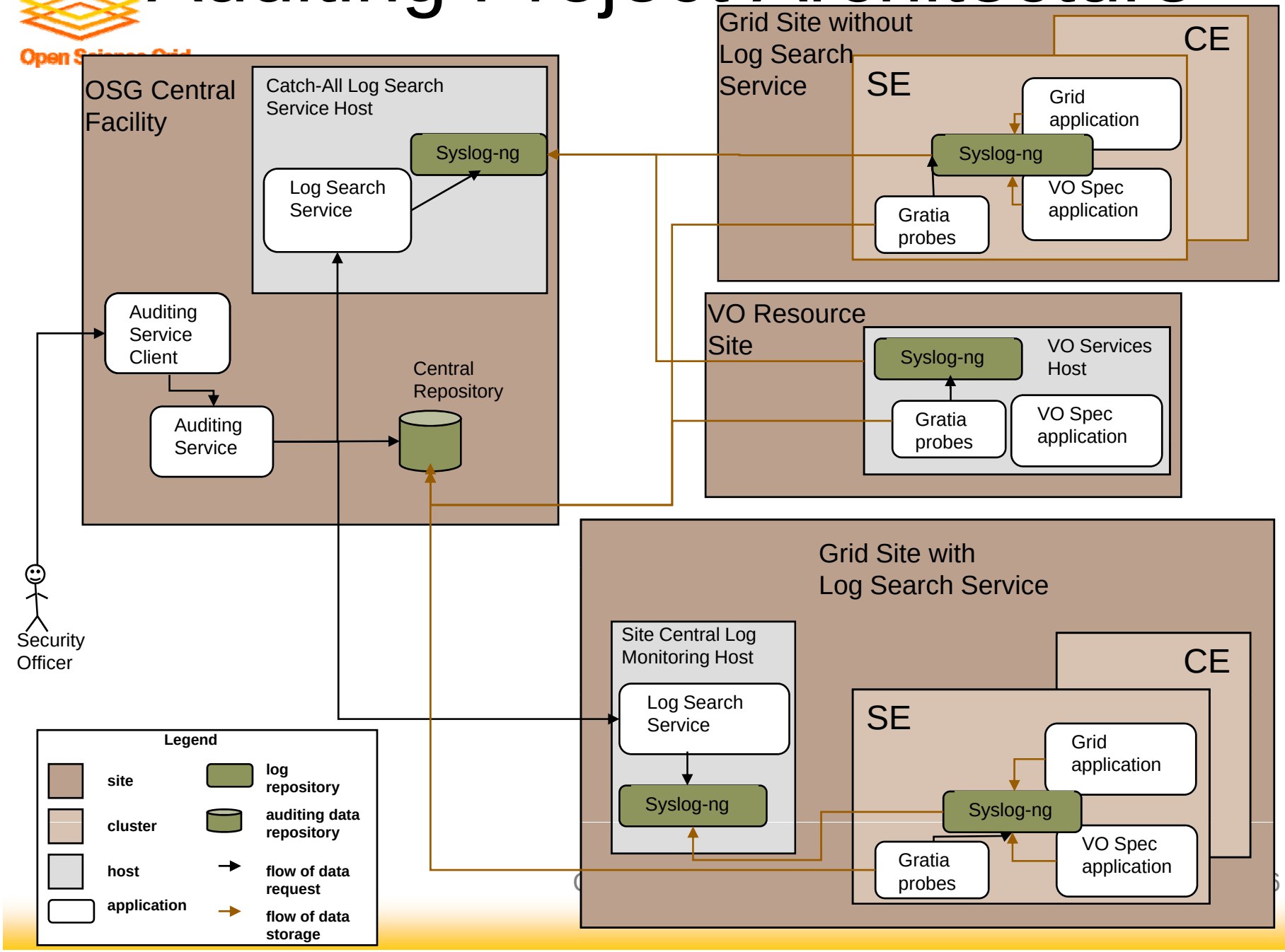
- The nature of the Grid cyberspace security vulnerabilities provides a motivation for creation of centralized service for real-time automated security assessment and forensic analysis.
- The usage patterns across the Grid may reveal adverse intentions while similar behavior may seem legitimate to any particular grid site or VO specific service.
- Use Cases:
  - should be able to determine if a specific, presumed to be stolen credential has been used to access Grid Sites or VO services
  - find out if there was an attempt to enter a site or service by scanning

Open Science Grid

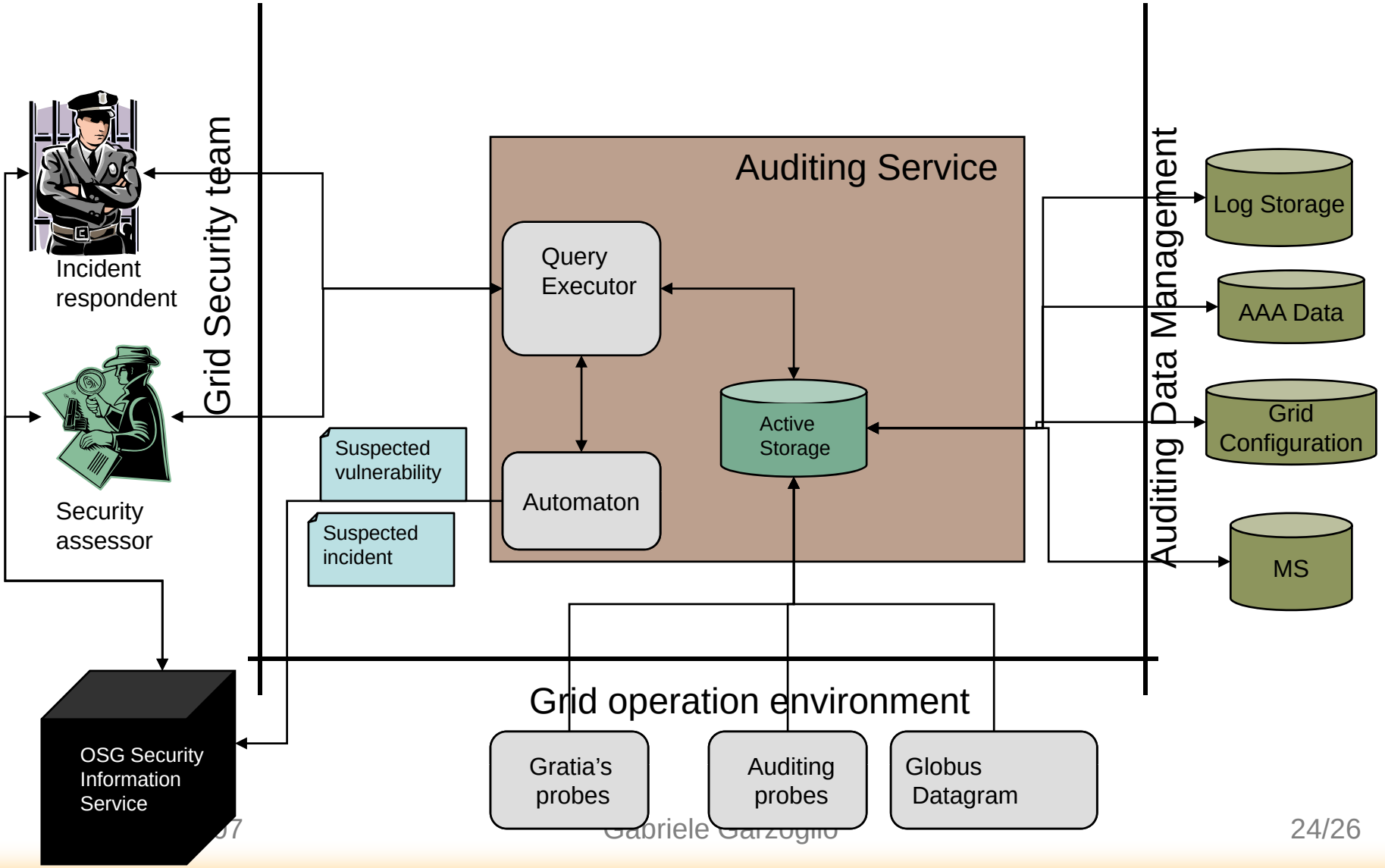
Project Goals

- Provide a global level auditing service to the OSG Community. The global auditing service is necessary to **assess the overall security condition of the OSG** across OSG sites and VO's specific services.
- Offer a **real-time automated security assessment and forensic analysis tools** that will satisfy the security requirements of OSG Staff, VO's, and sites participating in the OSG.
- Provide **flexible query interfaces** needed to *ad hoc* security investigations at the grid level.
- Interface OSG Information Management Project in order to **notify the appropriate officials** in case of discovery of unusual or suspicious gird usage.
- **Complement the existing site security processes** and help **drive further development of auditing collection software** used by Grid Sites.
- Focus on **integration and analysis of the**, possibly diverse and multiple-format, **information**.

Auditing Project Architecture



Auditing Project Context Diagram



Open Science Grid

Project Deliverables

- Provide a **review of the of auditing projects** within OSG, EGEE, CEDPS Troubleshooting project, and Globus Auditing (started)
- Provide a **evaluation summary the auditing tools** currently in use and/or available through **Open Source** (started)
- Provide the evaluation summary of **usability of the raw data collected by Gratia's probes for auditing** post-mortem analysis (started)
- Determine the **information model for service log files**, investigate log format transformations and log analysis capabilities
- **Achieve community consensus on the proposal** and encourage community collaboration on this project
- **Provide high level design of Auditing Service** (started)

Open Science Grid

Conclusion

- Security work in OSG is currently tackling both Policy and Middleware
- Policy work focuses on Management, Operation, and Technical controls to mitigate risk
- Middleware projects address User Registration, Access Authorization, Accounting (Gratia), and Auditing
- We want to collaborate with our European partners to achieve interoperations and share ideas